



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/688,456	10/16/2000	Craig L. Ogg	39778/RRT/S850	1637

23363 7590 04/19/2007
CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA, CA 91109-7068

EXAMINER

BACKER, FIRMIN

ART UNIT	PAPER NUMBER
----------	--------------

3621

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
2 MONTHS	04/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/688,456
Filing Date: October 16, 2000
Appellant(s): OGG ET AL.

MAILED

APR 19 2007

GROUP 3600

RAYMOND R. TABANDEH
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed July 13th, 2006 appealing from the Office action mailed September 23rd, 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,223,565

LEWIS ET AL

5-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-71 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by Lewis et al (U.S Patent No. 6,223,565).

3. As per claim 1, Lewis et al teach a cryptographic system for securing data on a computer network comprising a plurality of users coupled to the computer network and a plurality of cryptographic devices, each of the plurality of cryptographic devices remote from the plurality of users, and each of the plurality of cryptographic devices comprising a processor programmed to authenticate a the plurality of remote users on the computer network for secure processing of a value bearing item (VBI) a memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related the one of the plurality of users a cryptographic engine for cryptographically protecting data an interface for communicating with the computer network, and a module for processing value for the value bearing item, wherein each of the plurality of cryptographic devices is capable of authenticating any of the plurality of remote users, wherein each of the plurality of cryptographic devices is

Art Unit: 3621

capable of processing a VBI printing request from any of the plurality of remote users, and wherein each of the plurality of cryptographic devices is capable of generating indicia data for transmitting to any of the plurality of remote users (*see figs 1, 1A, 2, 3, 4A, 4B and their accompany text, column 6 lines 48-11 line 62*).

4. As per claims 2-40, Lewis et al teach a cryptographic system for securing data on a computer network that encompass all the limitation disclose claims and are related to the independent claim 1. Therefore, they are rejected under the same rationale.

5. As per claim 41, Lewis et al teach et al method for securing data on a computer network including a plurality of users and a plurality of cryptographic devices remote from the plurality of users comprising authenticating any one of the plurality of remote users by any one of the plurality of cryptographic devices, authorizing any one of the plurality of remote users for secure processing of a value bearing item by any one of a the plurality of cryptographic devices processing value for the value bearing item by the any one of the plurality of cryptographic devices; and storing a security device transaction data in a memory for ensuring authenticity and authority of one of the plurality users, wherein the security device transaction data is processed by any one of the plurality of cryptographic devices (*see figs 1, 1A, 2, 3, 4A, 4B and their accompany text, column 6 lines 48-11 line 62*).

Art Unit: 3621

6. As per claims 42-70, Lewis et al teach a cryptographic system for securing data on a computer network that encompass all the limitation disclose claims and are related to the independent claim 41. Therefore, they are rejected under the same rationale.

(10) Response to Argument

1. Applicants argue that the prior art fail to teach “a plurality of cryptographic devices remote fro the plurality of users.” Examiner respectfully disagrees with Applicant’s characterization of the prior art. Lewis teaches a customer 2n, a remote service provider (RSP) 4, and a third party seller of goods and/or services (TPS) 6. The letter "n" is used as a suffix to indicate "one of a plurality of n" such that there may be a plurality of n clients "2" in the system, but the discussion is generally for each client and extends to all clients, although not necessarily identically for each client. The client 2n has a Host system 10n and a PSD 20n which is resident on a server of RSP 4. The Host 10n accesses the remote PSD 20n via the Internet 30.

2. Applicants argue that the prior art fail to teach “a module for processing value for the value bearing item.” Examiner respectfully disagrees with Applicant’s characterization of the prior art. Lewis teaches a system wherein check purchasing is very similar to credit card purchasing. The difference is that the purchase server 190 does not need to go through the credit authorization server 400 to obtain any credit approval and typically has a suspense server 310 to enable check processing prior to issuance of postage. Because the check purchasing cannot be validated right away, the purchasing server 190 invokes the Persistence Service and Database

Art Unit: 3621

Service to update the database record, logging the transaction and updating the descending register in the PSD object. See Logging 196; Customer PSD 200 (increment); Master PSD 40 (decrement) in FIG. 3.

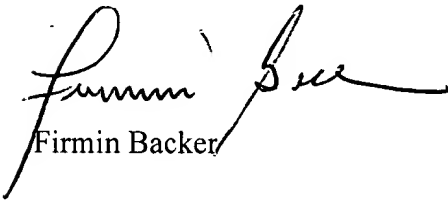
3. Applicants argue that the prior art fail to teach "a plurality of cryptographic devices is capable of authenticating any of the plurality of remote users." Examiner respectfully disagrees with Applicant's characterization of the prior art. Lewis teaches a client has a processor, a printer, a client authentication module, a module for issuing a transaction request, and a unique digital signature. The server has a network including a transaction server, a transaction database, a server authentication module, and a receipt generation module. An internet connection is used between the client and the server network. The transaction execution system includes Lewis teaches authentication, wherein the client authentication module and the server authentication modules communicate via the internet connection and are authenticated to each other. Lewis further teach a system the cryptographic module 12 is used to authenticate the customer 2n to the TPS 4 (hereinafter also referred to as "server 4"), the server 4 to the client 2n, and to manage the authentication key pair (public key/private key) that exists on the client 2. The main function of the client cryptographic module 12 is to protect the customer's private key from both intrusion and corruption. The customer's private key is used to authenticate the client 2 to the server 4.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,


Firmin Backer

Conferees:

Andrew Fisher



James Trammell

